PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-290396
(43)Date of publication of application : 04.10.2002

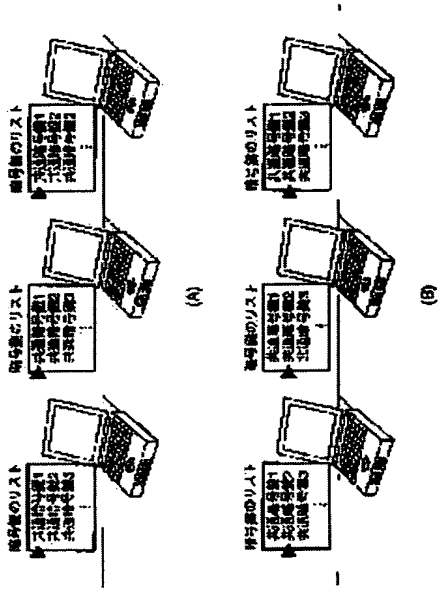
(51)IntCl H04L 9/16
H04L 9/08

(21)Application number : 2001-085823
(22)Date of filing : 23.03.2001

(71)Applicant : TOSHIBA CORP
(72)Inventor : SUZUKI NOBORU

(54) ENCRYPTION KEY UPDATE SYSTEM AND ENCRYPTION KEY UPDATE METHOD

(57)Abstract:
PROBLEM TO BE SOLVED : To provide an encryption key update system that can synchronously update encryption keys of all devices transmitting/receiving data without the need for users to make troublesome works such as entry of the encryption key and settings.
SOLUTION : The encryption key update system has distributed an encryption key list on which a plurality of encryption keys are described in advance to all devices encrypting data by using a common encryption key system, and also distributed a program to select one encryption key or more in the encryption key list on the basis of a prescribed rule to each device. For example, each device selects a 'common encryption key 1' for a period as an encryption key and automatically sets it to a communication environment. After that, each device aborts the 'common encryption key 1' on the border of a date and time and selects a 'common encryption key 2' for the encryption key and automatically sets it to the communication environment.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－290396
（P2002－290396A）
(43)公開日　平成14年10月４日(2002.10.4)

(51)Int.Cl.'	識別記号	ＦＩ	テーマコード'(参考)
Ｈ０４Ｌ　9/16		Ｈ０４Ｌ　9/00	６４３　５Ｊ１０４
9/08			６０１Ｅ

審査請求　未請求　請求項の数10　ＯＬ　（全９頁）

(21)出願番号　特願2001－85823(P2001－85823)

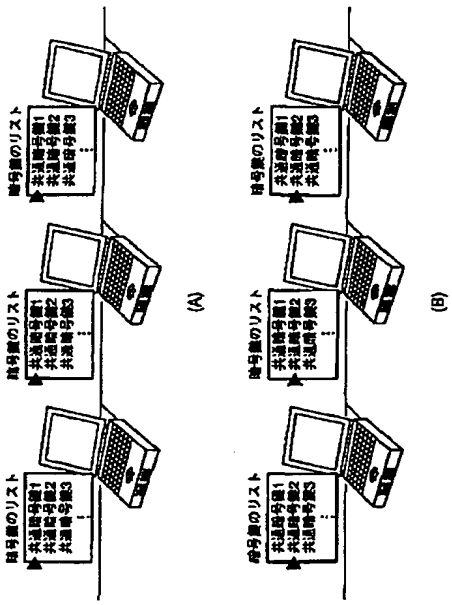
(22)出願日　平成13年３月23日(2001.3.23)

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(72)発明者　鈴木　昇
東京都青梅市末広町２丁目９番地　株式会社東芝青梅工場内
(74)代理人　100058479
弁理士　鈴江　武彦　（外６名）

Ｆターム(参考)　5J104 AA01 AA16 AA34 EA04 EA24
JA03 NA02 PA07

(54)【発明の名称】　暗号鍵更新システムおよび暗号鍵更新方法

(57)【要約】
【課題】ユーザに暗号鍵の入力や設定等の煩わしい作業を行わせることなく、データを送受信するすべての装置の暗号鍵を同期的に更新することを可能とした暗号鍵更新システム。
【解決手段】この暗号鍵更新システムでは、共通暗号鍵方式によるデータの暗号化を行うすべての装置に、予め複数の暗号鍵が記された暗号鍵リストを配布しておく。また、各装置には、所定の規則に基づき、この暗号鍵リストの中から１つ以上の暗号鍵を選択するプログラムも配布しておく。そして、たとえば、ある期間、各装置は、「共通暗号鍵１」を暗号鍵として選択し、それを通信環境に自動設定する。その後、ある日時を境に、各装置は、その「共通暗号鍵１」を破棄して「共通暗号鍵２」を暗号鍵として選択し、それを通信環境に自動設定する。



【特許請求の範囲】

【請求項１】　暗号化と復号とに同一の暗号鍵を用いる共通鍵方式によりデータを暗号化および復号しながら複数の装置が互いにデータを送受信する通信システムの暗号鍵更新システムであって、

前記各装置が、

複数の暗号鍵が記された電子的な暗号鍵リストを保持するリスト保持手段と、

予め定められた規則に基づき、前記リスト保持手段に保持された暗号鍵リストに記される複数の暗号鍵の中から１つ以上の暗号鍵を選択する選択手段とを具備したことを特徴とする暗号鍵更新システム。

【請求項２】　前記各装置が、

予め定められた規則に基づき、前記選択手段により選択された暗号鍵の有効期間を算出する有効期間算出手段と、

前記選択手段により暗号鍵が選択された時から前記有効期間算出手段により算出された期間が経過した時に、前記選択手段に新たな暗号鍵を選択させる暗号鍵更新手段とを具備したことを特徴とする請求項１記載の暗号鍵更新システム。

【請求項３】　前記選択手段は、前回選択した暗号鍵の中の少なくとも１つを再度選択することを特徴とする請求項１または２記載の暗号鍵更新システム。

【請求項４】　前記各装置が、

前記選択手段により暗号鍵が選択された時から予め定められた期間内に限り、その更新前の暗号鍵を復号用の暗号鍵の候補に加える時差調整手段を具備することを特徴とする請求項１または２記載の暗号鍵更新システム。

【請求項５】　前記各装置が、

前記暗号鍵リストを受信するリスト受信手段と、

前記リスト保持手段に保持された暗号鍵リストを前記リスト受信手段により受信された暗号鍵リストに更新するリスト更新手段とを具備することを特徴とする請求項１、２、３または４記載の暗号鍵更新システム。

【請求項６】　暗号化と復号とに同一の暗号鍵を用いる共通鍵方式によりデータを暗号化および復号しながら複数の装置が互いにデータを送受信する通信システムの暗号鍵更新方法であって、

前記各装置が、

複数の暗号鍵が記された電子的な暗号鍵リストを保持するステップと、

予め定められた規則に基づき、前記保持した暗号鍵リストに記される複数の暗号鍵の中から１つ以上の暗号鍵を選択するステップとを有することを特徴とする暗号鍵更新方法。

【請求項７】　前記各装置が、

予め定められた規則に基づき、前記選択された暗号鍵の有効期間を算出するステップと、

前記暗号鍵を選択した時から前記算出された期間が経過

した時に、新たな暗号鍵を選択するステップとを有することを特徴とする請求項６記載の暗号鍵更新方法。

【請求項８】　前記選択ステップは、前回選択した暗号鍵の中の少なくとも１つを再度選択することを特徴とする請求項６または７記載の暗号鍵更新方法。

【請求項９】　前記各装置が、

前記暗号鍵を選択した時から予め定められた期間内に限り、その更新前の暗号鍵を復号用の暗号鍵の候補に加えるステップを有することを特徴とする請求項６または７記載の暗号鍵更新方法。

【請求項１０】　前記各装置が、

前記暗号鍵リストを受信するステップと、

前記保持した暗号鍵リストを前記受信した暗号鍵リストに更新するステップとを有することを特徴とする請求項６、７、８または９記載の暗号鍵更新方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、たとえば無線通信回線を介してデータを送受信する通信システムの暗号鍵更新システムおよび暗号鍵更新方法に係り、特に、ユーザに暗号鍵の入力や設定等の煩わしい作業を行わせることなく、データを送受信するすべての装置の暗号鍵を同期的に更新することを可能とした暗号鍵更新システムおよび暗号鍵更新方法に関する。

【０００２】

【従来の技術】近年、データ通信技術の向上は目覚ましく、インターネットやイントラネットなどと称される通信システムが急速に普及している。また、最近では、赤外線や電波などによりデータを送受信する無線通信を利用した無線ＬＡＮ（Local AreaNetwork）をオフィス内に構築する企業も多くなってきている。この無線ＬＡＮは、ケーブルの敷設を必要としないために、たとえば組織の改編に伴うオフィス内のレイアウト変更などにも柔軟に対応することが可能である。

【０００３】赤外線や電波などにデータを搬送させる無線通信では、その漏洩を発生させ易いため、有線通信以上に、第３者によるデータの傍受や改ざん等を防ぐための対策が重要視される。このことから、従来より、データの暗号化という手法が広く採用されている。このデータの暗号化は、（１）共通暗号鍵方式、（２）公開暗号鍵方式のいずれか、あるいは、この２つの組み合わせによるものが現在のところ主流である。

【０００４】共通暗号鍵方式は、送信側（データを暗号化する側）と受信側（暗号化されたデータを復号する側）とが、予め共通の暗号鍵を持ち、この同一の暗号鍵を用いて暗号化および復号を行う方式である。一方、公開暗号鍵方式は、ある鍵から公開鍵と秘密鍵との２種類の鍵を生成し、公開鍵を予め送信側に配布しておく。そして、送信側は、この公開鍵を用いてデータを暗号化し、受信側は、この公開鍵と対になっている秘密鍵で復

号を実行する。また、この共通暗号鍵方式と公開暗号鍵方式との組み合わせは、共通暗号鍵方式における共通暗号鍵を公開暗号鍵方式によって授受するものである。

【０００５】このように、共通暗号鍵や公開鍵、秘密鍵を用いてデータの暗号化および復号を行うことにより、データの傍受や改ざんを防止することが可能となる。

【０００６】また、最近では、社内ＬＡＮに外出先等の遠隔地からアクセスしたいといった要望も多く、これに答えるために、たとえば加国ボーダー・ネットワーク・テクノロジー社や米国セキュリティダイナミクス社等がワンタイム・パスワード・システムと称されるユーザ認証システムを開発するに至っている。

【０００７】このワンタイム・パスワード・システムは、データを暗号化するものではないが、遠隔地からアクセスするユーザが正規のユーザかどうかを確認することによってネットワークのセキュリティを高めるためのシステムであり、たとえばネットワーク側のファイア・ウォールとモバイルコンピュータに接続される拡張ユニットなど、アクセスされる側とアクセスする側とで同じ時に同じ乱数を発生させる仕組みを持たせる。そして、ユーザは、たとえば１分ごとに発生・更新される乱数をパスワードとしてその拡張ユニットの入力装置に入力し、そのパスワードの承認を条件に、そのネットワークへのアクセスが許可される。

【０００８】つまり、このワンタイム・パスワード・システムでは、各パスワードがいわゆる使い捨てであるため、パスワードの盗難を考慮する必要がない。

【０００９】

【発明が解決しようとする課題】ところで、前述した共通暗号鍵方式によるデータの暗号化では、同じ鍵を長期間に渡って使い続けると、その暗号が破られる危険性が高くなってしまう。したがって、ある期間ごとに鍵を更新する作業が必要となってくる。

【００１０】しかしながら、たとえばＩＥＥＥ８０２．１１ｂ規格における無線ＬＡＮの暗号鍵は、４０ビット以内や１２８ビット以内での設定が可能であり、１２８ビットからなる暗号鍵を新たに配布・設定しようとすると、その作業は非常に煩雑である。そして、人手を介することから、たとえば設定ミスや暗号鍵自体の漏洩を誘発するおそれがあった。

【００１１】また、公開暗号鍵方式によるデータの暗号化や、共通暗号鍵方式と公開暗号鍵方式との組み合わせによる暗号化では、ハードウェアやファームウェアなど、ネットワークの下位層に処理をさせるには複雑すぎて実現困難であり、また、仮に実現できたとしても通信性能が著しく低下してしまうといった問題があった。

【００１２】一方、ワンタイム・パスワード・システムは、利用の度にパスワードを変える方式であるため、共通暗号鍵方式によるデータの暗号化のように、ある期間ごとに鍵を更新するといった作業は一切不要である。しかし、このワンタイム・パスワード・システムも、システムが発生させる乱数をその都度ユーザに入力させなければならないといった同様の問題を抱えている。

【００１３】この発明はこのような事情を考慮してなされたものであり、ユーザに暗号鍵の入力や設定等の煩わしい作業を行わせることなく、データを送受信するすべての装置の暗号鍵を同期的に更新することを可能とした暗号鍵更新システムおよび暗号鍵更新方法を提供することを目的とする。

【００１４】

【課題を解決するための手段】前述した目的を達成するために、この発明は、たとえば１年分の暗号鍵をすべての装置に予め配布しておき、各装置が、これらの中から暗号化および復号に用いる暗号鍵を他の装置と同じ規則で選択するようにしたものである。そして、そのために、この発明は、暗号化と復号とに同一の暗号鍵を用いる共通鍵方式によりデータを暗号化および復号しながら複数の装置が互いに情報を送受信する通信システムの暗号鍵更新システムであって、前記各装置が、複数の暗号鍵が記された電子的な暗号鍵リストを保持するリスト保持手段と、予め定められた規則に基づき、前記リスト保持手段に保持された暗号鍵リストに記される複数の暗号鍵の中から１つ以上の暗号鍵を選択する選択手段とを具備したことを特徴とする暗号鍵更新システムを提供する。

【００１５】この発明の暗号鍵更新システムにおいては、所定の規則に基づき、各装置が予め与えられた複数の暗号鍵の中から暗号化および復号に用いる暗号鍵を選択するため、その結果として、すべての装置が同期を取って暗号鍵を自動的に更新することが可能となり、ユーザに暗号鍵の入力や設定等の煩わしい作業を行わせることがない。

【００１６】また、この発明の暗号鍵更新システムは、前記各装置が、予め定められた規則に基づき、前記選択手段により選択された暗号鍵の有効期間を算出する有効期間算出手段と、前記選択手段により暗号鍵が選択された時から前記有効期間算出手段により算出された期間が経過した時に、前記選択手段に新たな暗号鍵を選択させる暗号鍵更新手段とを具備することが好ましい。これにより、暗号鍵の更新サイクルに不規則性を持たせることができ、セキュリティをより向上させることが可能となる。

【００１７】また、この発明の暗号鍵更新システムは、前記選択手段が、前回選択した暗号鍵の中の少なくとも１つを再度選択することが好ましい。これにより、たとえば更新前と更新後とで少なくとも１つは合致することになり、暗号鍵の更新時にもデータの送受信を中断させることがない。

【００１８】また、この発明の暗号鍵更新システムは、前記各装置が、前記選択手段により暗号鍵が選択された

時から予め定められた期間内に限り、その更新前の暗号鍵を復号用の暗号鍵の候補に加える時差調整手段を具備することが好ましい。これにより、複数の装置間での暗号鍵の更新タイミングのずれを適切な範囲内で吸収することが可能となる。

【００１９】また、この発明の暗号鍵更新システムは、前記各装置が、前記暗号鍵リストを受信するリスト受信手段と、前記リスト保持手段に保持された暗号鍵リストを前記リスト受信手段により受信された暗号鍵リストに更新するリスト更新手段とを具備することが好ましい。これにより、最初に暗号鍵リストを配布してシステムを起動させた後は、この暗号鍵リスト自体を暗号化して授受することができるようになり、以降、ユーザによる暗号鍵リストの配布や設定などを一切不要とすることが可能となる。

【００２０】

【発明の実施の形態】以下、図面を参照してこの発明の実施形態を説明する。

【００２１】図１は、この発明の実施形態に係る暗号鍵更新システムが適用される通信システムのネットワーク構成図である。

【００２２】図１に示すように、この通信システムは、有線ＬＡＮ１００にネットワーク管理サーバコンピュータ１と複数のアクセスポイント２とが接続される。また、各アクセスポイント２は、赤外線や電波などを利用して、パーソナルコンピュータ３との間に無線通信路を確立する。

【００２３】ネットワーク管理サーバコンピュータ１は、この通信システム全体の管理を司るものであり、後述する暗号鍵リストの配布などを実行する。また、アクセスポイント２は、パーソナルコンピュータ３を有線ＬＡＮ１００に接続するための装置であり、パーソナルコンピュータ３と同じ暗号鍵を保有し、この暗号鍵でデータの暗号化と復号とを行いながら、つまり共通暗号鍵方式による暗号化を行いながらパーソナルコンピュータ３との間でデータを送受信する。

【００２４】このアクセスポイント２とパーソナルコンピュータ３との双方に共有される暗号鍵は、たとえば４つまで一時に設定可能であり、複数の暗号鍵が設定された場合、送信側は、その中のどれかを用いて暗号化を行う。この時、送信側は、何番目の暗号鍵を使用したかを示す情報をパケットに格納して転送する。一方、受信側は、このパケットに格納された情報で示される番号の暗号鍵を用いて復号を実行する。

【００２５】そして、この通信システムに適用される暗号鍵更新システムは、このアクセスポイント２とパーソナルコンピュータ３との双方に共有される暗号鍵を、ユーザに暗号鍵の入力や設定等の煩わしい作業を行わせることなく、同期的に更新できるようにした点を特徴としており、以下、この点について詳述する。

【００２６】図２は、この暗号鍵更新システムで実行される暗号鍵の更新の概要を示すための概念図である。

【００２７】この暗号鍵更新システムでは、共通暗号鍵方式によるデータの暗号化を行うすべての装置、より具体的には、ここでは、すべてのアクセスポイント２およびパーソナルコンピュータ３に、予め複数の暗号鍵が記された暗号鍵リストを配布しておく。そして、各装置には、所定の規則に基づき、この暗号鍵リストの中から１つ以上の暗号鍵を選択するプログラムも配布しておく。

【００２８】たとえば図２（Ａ）に示すように、ある期間、各装置は、「共通暗号鍵１」を暗号鍵として選択し、それを通信環境に自動設定する。その後、図２（Ｂ）に示すように、ある日時を境に、各装置は、その「共通暗号鍵１」を破棄し、「共通暗号鍵２」を暗号鍵として選択し、それを通信環境に自動設定する。

【００２９】つまり、結果として、各装置の暗号鍵が同期的に更新されてセキュリティを高めることができ、かつ、ユーザに暗号鍵の入力や設定等の煩わしい作業を強いることもない。

【００３０】図３は、この通信システムを構成する各装置に備えられる暗号鍵更新システムに関わる構成を示すブロック図である。

【００３１】なお、この暗号鍵システムに関わる構成は、アクセスポイント２およびパーソナルコンピュータ３の双方に同じものが設けられるので、ここでは、パーソナルコンピュータ３を例に説明する。

【００３２】パーソナルコンピュータ３は、ＣＰＵ３１、システムメモリ３２、フロッピィディスク装置３３、磁気ディスク装置３４および無線信号送受信装置３５を有している。

【００３３】ＣＰＵ３１は、パーソナルコンピュータ３全体の制御を司るものであり、無線ＬＡＮ送受信制御プログラム３１１、暗号鍵管理プログラム３１２、アップデートプログラム３１３等の記述にしたがって、このパーソナルコンピュータ３を動作制御する。

【００３４】システムメモリ３２は、このパーソナルコンピュータ３の主記憶となるメモリデバイスであり、その時に実際にデータの暗号化および復号に用いられる暗号鍵３２１を格納するために利用される。

【００３５】フロッピィディスク装置３３および磁気ディスク装置３４は、このパーソナルコンピュータ３の外部記憶となるメモリデバイスであり、フロッピィディスク装置３３は、後述する暗号鍵リスト３４１が格納された頒布用のフロッピィディスクからこれらを読み出すために利用される。一方、磁気ディスク装置３４は、フロッピィディスク装置３３によりフロッピィディスクから読み出された暗号鍵リスト３４１を格納するために利用される。この暗号鍵リスト３４１は、図２を参照しながら説明した、予め複数の暗号鍵が記された暗号鍵リストである。

【００３６】そして、無線信号送受信装置３５は、データを搬送するための赤外線信号をアクセスポイント２に向けて送信し、あるいは、アクセスポイント２から送信された赤外線信号を受信するためのものである。

【００３７】ここで、このパーソナルコンピュータ３が、無線信号送受信装置３５を介してアクセスポイント２にデータを送信する場合、および、無線信号送受信装置３５を介してアクセスポイント２からデータを受信する場合を考える。

【００３８】データを送信する場合、無線ＬＡＮ送受信制御プログラム３１１は、システムメモリ３２に格納されたいずれかの暗号鍵３２１を用いてデータを暗号化し、この暗号化されたデータを無線信号送受信装置３５を介してアクセスポイント２に送信する。この時、何番目の暗号鍵３２１を使用したのかを示す情報をパケットに格納しておく。一方、データを受信する場合、無線ＬＡＮ送受信制御プログラム３１１は、システムメモリ３２に格納された暗号鍵３２１の中のパケットで指定される番号の暗号鍵３２１を用いてデータを復号する。

【００３９】つまり、このパーソナルコンピュータ３におけるアクセスポイント２との間のデータの送受信では、システムメモリ３２に格納された暗号鍵３２１の管理が非常に重要であることがわかる。

【００４０】そこで、次に、暗号鍵管理プログラム３１２が実行する、この暗号鍵３２１の更新について説明する。

【００４１】まず、図４を参照して、この暗号鍵管理プログラム３１２による暗号鍵の更新の第１の動作原理を説明する。

【００４２】いま、暗号鍵リスト３４１には、暗号鍵（１）～（ｎ）の複数の暗号鍵が記されており、また、システムメモリ３２には、当初、暗号鍵（１）～（４）が暗号鍵３２１として設定されているものと想定する。

【００４３】ある期間の経過後、暗号鍵管理プログラム３１２は、予め定められた規則に基づき、システムメモリ３２の暗号鍵３２１から既存の暗号鍵（１）と、磁気ディスク装置３４の暗号鍵リスト３４１から暗号鍵（５）～（７）とを選択し、これをシステムメモリ３２に新たな暗号鍵３２１として再設定する。

【００４４】さらにある期間の経過後、暗号鍵管理プログラム３１２は、予め定められた規則に基づき、システムメモリ３２の暗号鍵３２１から既存の暗号鍵（５）と、磁気ディスク装置３４の暗号鍵リスト３４１から暗号鍵（１８）～（２０）とを選択し、これをシステムメモリ３２に新たに暗号鍵３２１として再設定する。

【００４５】同様に、さらにある期間の経過後、暗号鍵管理プログラム３１２は、予め定められた規則に基づき、システムメモリ３２の暗号鍵３２１から既存の暗号鍵（１９）と、磁気ディスク装置３４の暗号鍵リスト３４１から暗号鍵（３２）～（３４）とを選択し、これをシステムメモリ３２に新たに暗号鍵３２１として再設定する。

【００４６】つまり、暗号鍵管理プログラム３１２は、４つの暗号鍵の中の１つは更新前と更新後とで重複させることにより、この暗号鍵の更新時にデータの送受信を中断させることを防止する。

【００４７】なお、この選択時の規則として、暗号鍵管理プログラム３１２は、暗号鍵リスト３４１の端から順番に暗号鍵を選択していってもよいが、その順番に不規則性を持たせれば、さらにセキュリティを高めることが可能である。この不規則性を持たせる方法としては、たとえばパーソナルコンピュータ３のシステム時刻を取得し、この取得したシステム時刻をもとに予め定められた関数演算を実行して選択すべき暗号鍵を決定するなどすればよい。

【００４８】また、暗号鍵管理プログラム３１２は、この暗号鍵の更新を予め定められた期間ごとに行ってもよいが、そのサイクルにも不規則性を持たせれば、さらにセキュリティを高めることが可能である。この不規則性を持たせる方法としては、たとえばパーソナルコンピュータ３のシステム時刻を取得し、この取得したシステム時刻をもとに予め定められた関数演算を実行して各暗号鍵の有効期間を決定するなどすればよい。

【００４９】次に、図５を参照して、この暗号鍵管理プログラム３１２による暗号鍵の更新の第２の動作原理を説明する。

【００５０】いま、暗号鍵リスト３４１には、暗号鍵（１）～（ｎ）の複数の暗号鍵が記されており、また、システムメモリ３２には、当初、暗号鍵（１）～（２）が暗号鍵３２１として設定されているものと想定する。つまり、ここでは、一時に設定可能な数であるたとえば４つのうちの半数の２つの暗号鍵を設定する。

【００５１】ある期間の経過後、暗号鍵管理プログラム３１２は、予め定められた規則に基づき、磁気ディスク装置３４の暗号鍵リスト３４１から暗号鍵（５）～（６）を選択し、これをシステムメモリ３２に新たな暗号鍵３２１として再設定する。

【００５２】これに伴い、無線ＬＡＮ送受信制御プログラム３１１は、データを暗号化する際に用いる暗号鍵の候補を暗号鍵（５）～（６）の２つとする。しかし、無線ＬＡＮ送受信制御プログラム３１１は、この暗号鍵が更新された時から予め定められた期間内に限り、データを復号する際に用いる暗号鍵の候補を暗号鍵（５）～（６）の２つに更新前の暗号鍵（１）～（２）を加えた合計４つとする。

【００５３】さらにある期間の経過後、暗号鍵管理プログラム３１２は、予め定められた規則に基づき、磁気ディスク装置３４の暗号鍵リスト３４１から暗号鍵（１８）～（１９）を選択し、これをシステムメモリ３２に新たな暗号鍵３２１として再設定する。これに伴い、無

線ＬＡＮ送受信制御プログラム３１１は、データを暗号化する際に用いる暗号鍵の候補を暗号鍵（１８）～（１９）の２つとし、この暗号鍵が更新された時から予め定められた期間内に限り、データを復号する際に用いる暗号鍵の候補を暗号鍵（１８）～（１９）の２つに更新前の暗号鍵（５）～（６）を加えた合計４つとする。

【００５４】同様に、さらにある期間の経過後、暗号鍵管理プログラム３１２は、予め定められた規則に基づき、磁気ディスク装置３４の暗号鍵リスト３４１から暗号鍵（３２）～（３３）を選択し、これをシステムメモリ３２に新たな暗号鍵３２１として再設定し、無線ＬＡＮ送受信制御プログラム３１１は、データを暗号化する際に用いる暗号鍵の候補を暗号鍵（３２）～（３３）の２つとするとともに、この暗号鍵が更新された時から予め定められた期間内に限り、データを復号する際に用いる暗号鍵の候補を暗号鍵（３２）～（３３）の２つに更新前の暗号鍵（１８）～（１９）を加えた合計４つとする。

【００５５】つまり、暗号鍵管理プログラム３１２は、暗号鍵の更新を更新前と更新後とで重複することなく実行するが、無線ＬＡＮ送受信制御プログラム３１１が、更新前の暗号鍵を予め定められた期間内に限り許容することにより、複数の装置間での暗号鍵の更新タイミングのずれを適切な範囲内で吸収する。そして、このために、暗号鍵管理プログラム３１２は、暗号鍵の設定数を一時に取り扱い可能な数の半数以下とする。

【００５６】このように、この暗号鍵更新システムでは、たとえば１年分の暗号鍵をすべての装置に予め配布しておき、各装置が、これらの中から暗号化および復号に用いる暗号鍵を他の装置と同じ規則で選択するようにしたことにより、ユーザに暗号鍵の入力や設定等の煩わしい作業を行わせることなく、データを送受信するすべての装置の暗号鍵を同期的に更新することを可能とする。

【００５７】次に、図６および図７を参照して、この暗号鍵更新システムの動作手順を説明する。

【００５８】図６は、暗号鍵管理プログラム３１２の動作手順を説明するためのフローチャートである。

【００５９】暗号鍵管理プログラム３１２は、まず、このパーソナルコンピュータ３のシステム時刻を取得する（ステップＡ１）。システム時刻を取得すると、暗号鍵管理プログラム３１２は、その取得したシステム時刻をもとに暗号鍵選択用に予め与えられた関数演算を実行し、磁気ディスク装置３４に格納された暗号鍵リスト３４１の中から新たな暗号鍵を選択する（ステップＡ２）。

【００６０】新たな暗号鍵を選択すると、暗号鍵管理プログラム３１２は、その選択した暗号鍵をシステムメモリ３２に暗号鍵３２１として設定する（ステップＡ３）。そして、暗号鍵管理プログラム３１２は、先に取得したシステム時刻をもとに有効期間算出用に予め与えられた関数演算を実行し、この新たな暗号鍵の有効期間を算出する（ステップＡ４）。

【００６１】最後に、暗号鍵管理プログラム３１２は、その算出した有効期間後に自身を再起動するための起動タイマを設定し（ステップＡ５）、この処理を終了する。

【００６２】図７は、無線ＬＡＮ送受信制御プログラム３１１の復号時における動作手順を説明するためのフローチャートである。

【００６３】無線ＬＡＮ送受信制御プログラム３１１は、無線信号送受信装置３５を介してアクセスポイント２からのデータを受信すると、システムメモリ３２に設定された暗号鍵の中のパケットで指定された番号の暗号鍵を用いてこのデータの復号を試みる（ステップＢ１）。

【００６４】この復号が成功すると（ステップＢ２のＹＥＳ）、無線ＬＡＮ送受信制御プログラム３１１による復号処理は終了であるが、一方、失敗すると（ステップＢ２のＮＯ）、無線ＬＡＮ送受信制御プログラム３１１は、システムメモリ３２に設定された暗号鍵３２１の更新から予め定められた期間内かどうかを調べる（ステップＢ３）。

【００６５】予め定められた期間内であれば（ステップＢ３のＹＥＳ）、無線ＬＡＮ送受信制御プログラム３１１は、今度は、更新前の旧暗号鍵の中のパケットで指定された番号の旧暗号鍵を用いてこのデータの復号を試みる（ステップＢ４）。

【００６６】そして、復号が成功すれば（ステップＢ７のＹＥＳ）、無線ＬＡＮ送受信制御プログラム３１１による復号処理は終了となり、一方、失敗するか（ステップＢ５のＮＯ）、あるいは、暗号鍵３２１の更新から予め定められた期間内でなかったとき（ステップＢ３のＮＯ）、無線ＬＡＮ送受信制御プログラム３１１は、アクセスポイント２にエラー返答を通知する（ステップＢ６）。

【００６７】なお、この図７で示した無線ＬＡＮ送受信制御プログラム３１１の復号時における動作手順は、暗号鍵管理プログラム３１２が図５に示した第２の動作原理で暗号鍵を更新する場合のものであり、暗号鍵管理プログラム３１２が図４に示した第１の動作原理で暗号鍵を更新する場合には、ステップＢ２における復号が失敗した時点で、ステップＢ６のエラー返答の通知を行えばよい。

【００６８】ところで、この暗号鍵リスト３４１を配布してシステムを起動させた後は、この暗号鍵リスト３４１自体を暗号化して授受することができるようになる。したがって、これ以降は、頒布用のフロッピィディスクに暗号鍵リスト３４１を格納して配布し、各装置側でフロッピィディスク装置３３により読み出して設定するな

どといったことを一切不要とすることが可能となる。そして、そのために、この暗号鍵更新システムでは、アップデートプログラム３１３を準備する。

【００６９】ネットワーク管理サーバコンピュータ１から送信される暗号鍵リストが無線信号送受信部装置３５により受信されると、まず、無線ＬＡＮ送受信制御プログラム３１１が、アクセスポイント２によって暗号化された暗号鍵リストの復号を実行する。そして、この復号された暗号鍵リストは、アップデートプログラム３１３に転送され、アップデートプログラム３１３によって、磁気ディスク装置３４の暗号鍵リスト３４１の更新が実行される。

【００７０】また、セキュリティをより高めるために、このアップデートプログラム３１３に、暗号鍵管理プログラム３１２の更新機能をもたせることも有効である。つまり、ネットワーク管理サーバコンピュータ１から暗号化された新たな暗号鍵管理プログラムを送信し、この暗号化された新たな暗号鍵管理プログラムを無線ＬＡＮ送受信制御プログラム３１１に復号させた後、アップデートプログラム３１３に暗号鍵管理プログラム３１２の更新を実行させる。これにより、暗号鍵の選択規則も人手を介さずに更新できることになり、かつ、暗号が破られる危険性を低くすることが可能となる。

【００７１】

【発明の効果】以上、詳述したように、この発明によれば、たとえば１年分の暗号鍵をすべての装置に予め配布しておき、各装置が、これらの中から暗号化および復号に用いる暗号鍵を他の装置と同じ規則で選択するようにしたため、その結果として、すべての装置が同期を取って暗号鍵を自動的に更新することが可能となり、ユーザに暗号鍵の入力や設定等の煩わしい作業を行わせることがない。

【００７２】また、暗号鍵の更新サイクルに不規則性を持たせることにより、セキュリティをより向上させることが可能となる。

【００７３】さらに、たとえば更新前と更新後とで暗号鍵を少なくとも１つは重複させ、あるいは、予め定めら＊れた期間内に限り更新前の暗号鍵を復号用の暗号鍵の候補に加えることにより、暗号鍵の更新時にもデータの送受信を中断させることを防止し、あるいは、複数の装置間での暗号鍵の更新タイミングのずれを適切な範囲内で吸収することを可能とする。

【図面の簡単な説明】

【図１】この発明の実施形態に係る暗号鍵更新システムが適用される通信システムのネットワーク構成図。

【図２】同実施形態の暗号鍵更新システムで実行される暗号鍵の更新の概要を示すための概念図。

【図３】同実施形態の通信システムを構成する各装置に備えられる暗号鍵更新システムに関わる構成を示すブロック図。

【図４】同実施形態の暗号鍵管理プログラムによる暗号鍵の更新の第１の動作原理を説明するための図。

【図５】同実施形態の暗号鍵管理プログラムによる暗号鍵の更新の第２の動作原理を説明するための図。

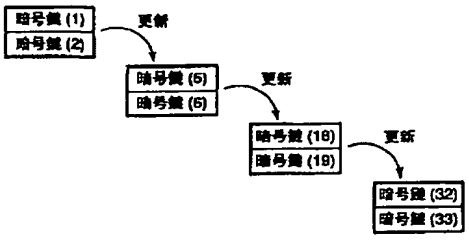
【図６】同実施形態の暗号鍵管理プログラムの動作手順を説明するためのフローチャート。

【図７】同実施形態の無線ＬＡＮ送受信制御プログラムの復号時における動作手順を説明するためのフローチャート。

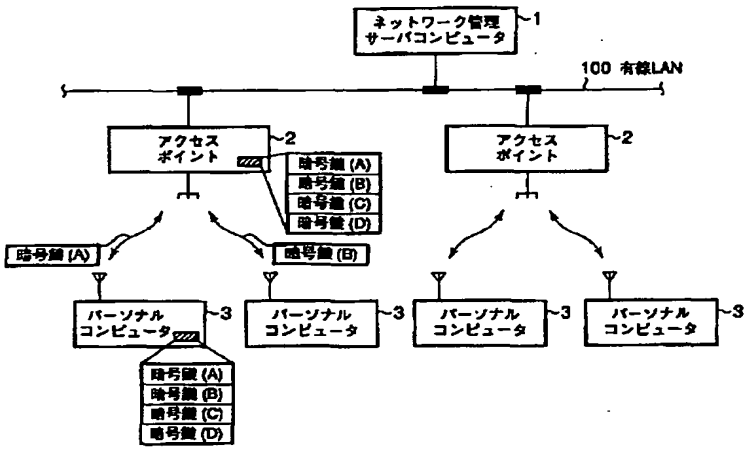
【符号の説明】

１…ネットワーク管理サーバコンピュータ
２…アクセスポイント
３…パーソナルコンピュータ
３１…ＣＰＵ
３２…システムメモリ
３３…フロッピィディスク
３４…磁気ディスク装置
３５…無線信号送受信装置
１００…有線ＬＡＮ
３１１…無線ＬＡＮ送受信制御プログラム
３１２…暗号鍵管理プログラム
３１３…アップデートプログラム
３２１…暗号鍵
３４１…暗号鍵リスト

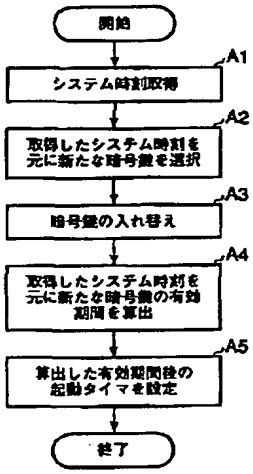
【図５】



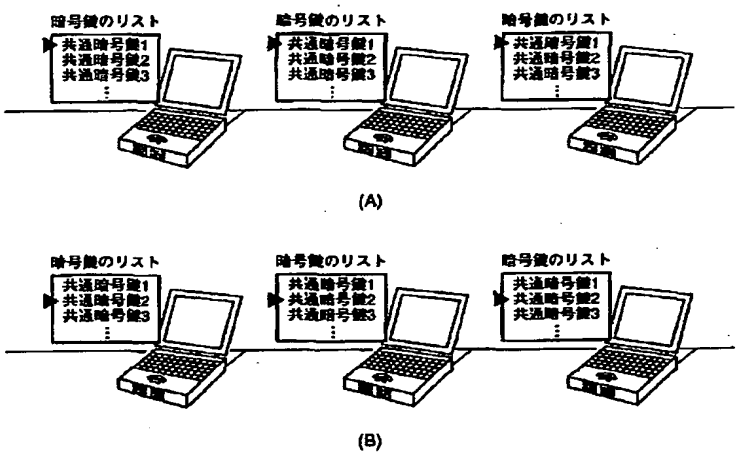
【図１】


ネットワーク管理
サーバコンピュータ
1
100 有線LAN
アクセス
ポイント
2
暗号鍵 (A)
暗号鍵 (B)
暗号鍵 (C)
暗号鍵 (D)
パーソナル
コンピュータ
3

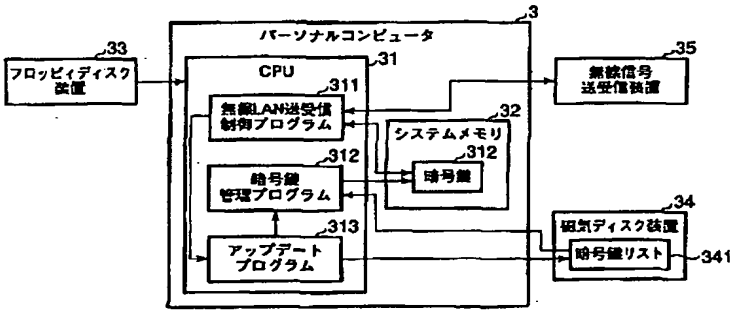
【図６】


開始
A1
システム時刻取得
A2
取得したシステム時刻を
元に新たな暗号鍵を選択
A3
暗号鍵の入れ替え
A4
取得したシステム時刻を
元に新たな暗号鍵の有効
期間を算出
A5
算出した有効期間後の
起動タイマを設定
終了

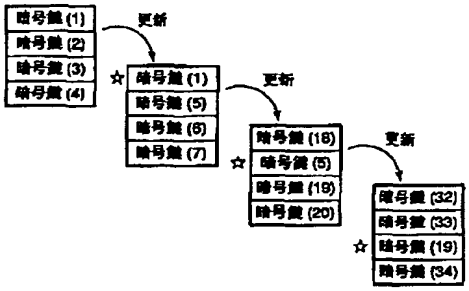
【図２】


暗号鍵のリスト
共通暗号鍵1
共通暗号鍵2
共通暗号鍵3
(A)
(B)

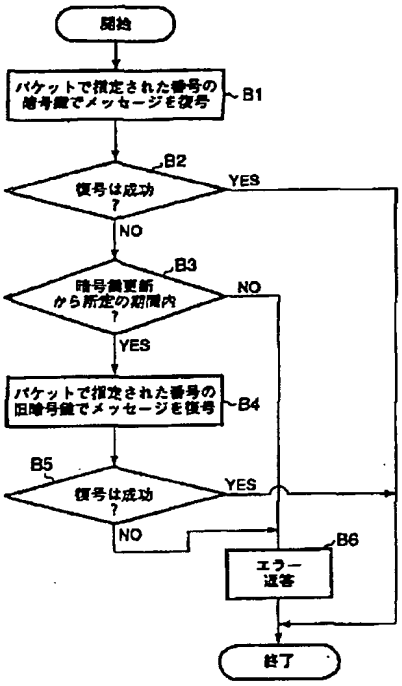
【図３】


パーソナルコンピュータ
3
フロッピィディスク
装置
33
CPU
31
無線LAN送受信
制御プログラム
311
システムメモリ
32
暗号鍵
312
暗号鍵
管理プログラム
アップデート
プログラム
313
無線信号
送受信装置
35
磁気ディスク装置
34
暗号鍵リスト
341

【図４】


暗号鍵(1)
暗号鍵(2)
暗号鍵(3)
暗号鍵(4)
更新
☆暗号鍵(1)
暗号鍵(5)
暗号鍵(6)
暗号鍵(7)
更新
暗号鍵(16)
☆暗号鍵(5)
暗号鍵(19)
暗号鍵(20)
更新
暗号鍵(32)
暗号鍵(33)
☆暗号鍵(19)
暗号鍵(34)

【図７】


開始
パケットで指定された番号の暗号鍵でメッセージを復号
B1
B2
復号は成功？
YES
NO
B3
暗号鍵更新から所定の期間内？
NO
YES
パケットで指定された番号の旧暗号鍵でメッセージを復号
B4
B5
復号は成功？
YES
NO
B6
エラー返答
終了